REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-04-2012	Master of Military Studies Research Paper	Sep 2011 - Apr 2012

4. TITLE AND SUBTITLE
AWAITING THE CYBER 9/11

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Clifford S. Magee

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

United States is again awaiting a very public, catastrophic event before awakening to the threat of cyber warfare. Before the events on 9/11, terrorism was largely considered a crime problem handled by the law enforcement and the intelligence community. Local police and the FBI would arrest terror suspects and the CIA was heavily engaged in intelligence collection against terrorist organizations. Terrorism was not a DOD focus of effort. The events of 9/11 changed the focus for the DOD, and the DOD now fills a huge anti-terror role because of the ferocity of the 9/11 attacks. Similar to 9/11, adversaries we face today will exploit the nation's cyber defenses in an effort to destroy the American way of life.

15. SUBJECT TERMS
Cyber Domain, Cyber Battlespace, Web as a Weapon, Cyber Common Operating Picture, Cyber Reform. Cyber Cloud Cyber Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University / Command and Staff Col
Unclass	Unclass	Unclass	UU	28	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

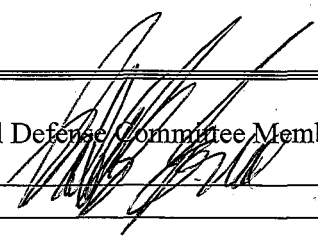
MASTER OF MILITARY STUDIES

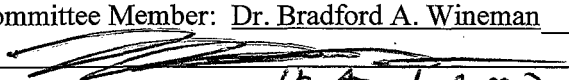
AWAITING THE CYBER 9/11

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Clifford S. Magee, USMC

AY 11-12

Mentor and Oral Defense Committee Member: Dr. Robert B. Bruce
Approved: 
Date: 12 April 2012

Oral Defense Committee Member: Dr. Bradford A. Wineman
Approved: 
Date: 13 April 2012

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Page

ACKNOWLEDGMENTS

I would like to thank my beautiful wife, Sophie Magee, for her unlimited patience and support. She has been my "center of gravity". Many thanks also go to my children, Dylan, Tyler, Brady, and Madelyn for bringing much needed fun and entertainment. The amount and quality of time we spent together this year will be one of the highlights of my life.

I would like to thank my brother-in-law, Craig Tadken, for his time, humor, mentorship, and extraordinary proofreading abilities. He ensured that I didn't embarrass myself with poor grammar or syntax. He also put up with some of my ridiculously short and self-imposed deadlines. I certainly would not have been successful without his assistance.

I would also like to thank my brother, Kevin Magee, and sister, Pam Tadken, for their intellectual contribution and uncompromising support to the family. Through great times and some difficult times they have been the foundation that has allowed for their siblings, children, nephews, and nieces to continue to thrive.

Finally I would like to thank my thesis advisor, Dr. Robert B. Bruce, and faculty advisor, LtCol Karl C. Rohr for their time, ideas, and exceptional teaching abilities.

EXECUTIVE SUMMARY

Title: Awaiting the Cyber 9/11

Author: Major Clifford S. Magee, United States Marine Corps

Thesis: The national security, economy and critical infrastructure of the United States is under cyber attack every day. Some of the attacks are from nation-states like China and Russia, while others are from non-state players like terrorist organizations, criminal gangs, teenage hackers, or anarchists. In order to protect the financial systems, power grids, telecommunications, water supplies, intellectual property and military communications of the United States; the United States Government needs to designate the Department of Defense (DOD) as the lead organization in preventing, detecting and recovering from cyber attacks.

Discussion: United States is again awaiting a very public, catastrophic event before awakening to the threat of cyber warfare. Before the events on 9/11, terrorism was largely considered a crime problem handled by the law enforcement and the intelligence community. Local police and the FBI would arrest terror suspects and the CIA was heavily engaged in intelligence collection against terrorist organizations. Terrorism was not a DOD focus of effort. The events of 9/11 changed the focus for the DOD, and the DOD now fills a huge anti-terror role because of the ferocity of the 9/11 attacks. Similar to 9/11, adversaries we face today will exploit the nation's cyber defenses in an effort to destroy the American way of life.

Conclusion: Cyber war has already begun. Its costs are low and its impacts can be existential. The most target-rich country in the world is the United States, but the military networks are not the prime targets, the prime targets are in the civilian sector. Leon Panetta, the Secretary of Defense, warned "the next Pearl Harbor will be a cyber attack." Just as the attack on Pearl Harbor finally galvanized the United States' government and public sectors after years of aggressive Japanese actions throughout the Pacific, Leon Panetta's warning is *deja vu*. State and non-state actors have been performing cyber operations against the United States at an alarming rate and the loss of intellectual property and United States Government secrets has weakened the United States defense posture and negated its technological advantages, but it seems that the "sleeping giant" of the United States is again awaiting a very public, catastrophic event before awakening.

Before a major attack occurs, the United States Government should appoint the DOD as the lead in defending the cyber domain. The DOD and private sector are interdependent on the cyber domain for operations and should coordinate to defend this vital capability. The DOD has the resident intellectual and technological capabilities required to fuse the information of attacks from both the private and public cyber domains. Assisted by regulation and new technologies, such as cloud computing, the DOD should lead efforts to prevent, detect, and recover from cyber attacks against government and critical infrastructure. By leveraging innovations such as "cloud computing," ensuring compliance of best security practices and providing an offensive cyber capability, the DOD can minimize the threat to the nation's security and prosperity.

Table of Contents

Page

INTRODUCTION

Enemies of the United States no longer need to launch missiles or fly airplanes into buildings to successfully attack the United States. A new weapon has been introduced into the world's arsenal, and that weapon has no boundaries, no rules, little cost and monstrous potential. The new weapon is cyber warfare.

The national security, economy, and critical infrastructure of the United States is under cyber attack every day.[1] Some of the attacks are from nation-states like China and Russia, while others are from non-state players like terrorist organizations, criminal gangs, teenage hackers, or anarchists.[2] In order to protect the financial systems, power grids, telecommunications, water supplies, intellectual property and military communications of the United States, the United States Government needs to designate the Department of Defense (DOD) as the lead organization in preventing, detecting, and recovering from cyber attacks.

In 2009, the *Wall Street Journal* reported that Chinese hackers had successfully gained access to the control systems for the United States electric power grid and created secret openings.[3] There was no monetary value in gaining control of the electrical grid, nor was there any intelligence value that would justify cyber espionage.[4] The only point to penetrating the grid's controls was to be prepared to combat American military superiority with an asymmetrical cyber war.[5] The Chinese had created a capability that could cause power outages across the United States and possibly cause nuclear incidents without firing a shot. The victims of the intrusion were unaware their systems had been compromised and remained so until the intrusions were detected by the United States Government intelligence community.[6] What would the United States have done if it discovered that China had been laying explosive charges throughout the national electrical grid system?[7]

The threats posed in the cyber domain are, in fact, an existential threat to the security and prosperity of the nation. Currently, the United States does not have an organization that has the capabilities or authorities to oversee cyber security for the United States Government and private sector. To develop this capability, the United States needs to undergo a paradigm shift on how it views the cyber domain.

THE CYBER DOMAIN

In 1911, British naval theorist Julian Corbett in his book *Principles of Maritime Strategy* stated that the British Navy was necessary because it provided sea power to protect the goods and services that travel on the sea.[9] The British economy was based on trade, and the sea lanes for communications and trade were extraordinarily important for the security and prosperity of Britain. Today, the security and prosperity of the United States is dependent on cyber trade routes, but cyber space is vulnerable to attack; signals and information can be intercepted, interrupted, and exploited. The United States needs to develop a strategy to defend the cyber domain similar to the strategies it developed for defending the air, land, and sea domains.

Defense of the United States air, sea, and land domains is accomplished by the integrated efforts of the DOD. Defense of the air trade routes is not the responsibility of the Federal Aviation Administration or American Air Lines; it is the the Department of Defense's (DOD) responsibility.[10] Similarly, Maersk Lines is not responsible for defense of the sea domain, but in the cyber domain every American company is responsible for its own defense without support from the Government. The United States government does not yet have a lead organization to defend all government networks from attacks, much less assist with defending the private sector. The DOD needs to be assigned the responsibility of defending the cyber domain with assistance from the Department of Homeland Security, the Intelligence Community, and the private sector.

The DOD needs to develop an active layered cyber defense with offensive and defensive capabilities. Currently, most cyber defensive strategies rely on firewalls to block attacks. This method is similar to the post World War I French creation of the Maginot Line.[11] The Maginot Line was an expensive defensive measure designed to keep the Germans out of France, but in 1940 the wall didn't work. The Maginot Line was a single capability; the strategy of the line lacked both a layered defensive structure as well as the offensive capability needed for defense. To avoid the cyber Maginot line, the United States needs both a layered, integrated defenses as well as an offensive capability.

DEFINING THE BATTLESPACE

The cyber domain has been created in a short period of time and has not had the level of scrutiny that other battle domains have had. The sea and land domains have had thousands of years of discussion to create generally accepted definitions. The air domain has had approximately 100 years of dedicated study. The discussions involving cyber as a battle domain are still nascent.

The rapid evolution and ever increasing complexity of the cyber domain has not yet allowed for agreement as to what the definition of the cyber domain should be. Some define cyberspace as "the internet;" the CIA's definition to congress is that "cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography."[12] The official DOD definition of cyber as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers,"[13] is the most thorough definition, but is so all-

encompassing that it is difficult to comprehend. Understanding the characteristics of cyber space will assist in understanding the definition of the cyber domain.

Cyber space is a manmade domain created by information technologies. Cyber space is composed of radio waves, cell phones, fiber optic cables, satellites, laser beams, software, firmware, and anything that can be linked together to create a network.[14] Some characteristics required to support cyber space are that it requires electronic components, electricity, and an infrastructure to connect it all together.

Understanding the characteristics of cyber space supports an understanding of cyber warfare. Cyber warfare is generally divided into two core operational capabilities: Computer Network Operations (CNO) and Electromagnetic Warfare (EW).

CNO is a broad term that encapsulates three subcategories: network defense, network exploitation, and network attack.

- Network defensive actions are used to protect computers and networks.[15]
- Network exploitation actions are used to gain information from other computer assets.[16]
- Network attack actions are taken to disrupt, deny, degrade, or destroy information or capability.[17]

Network defense operations are generally divided into passive and active defenses. Network defense information assurance operations are passive and designed to protect, monitor, analyze, and detect incidents on a network. Network defense response actions are actions that are both passive and active and are designed to respond to unauthorized activity.

In the United States, network defense information assurance is the most common method used to protect networks. An analogy for network defense information assurance practices is placing camouflage netting, barbed wire, and sandbags to protect a position. Network defense

information assurance efforts are generally 80 percent effective in defending against intrusions,[18] but Symantec, a computer security company, "identified more than 240 million distinct new malicious programs in 2009, a 100% increase over 2008."[19] Using the 80 percent efficacy rate still leaves 48 million vulnerabilities to threaten networks.

In 2008, the DOD suffered a major failure in its network defense.[20] It started when an infected flash drive was placed into a United States military laptop at a base in the Middle East.[21] The flash drive was placed in the parking lot of a DOD facility by a foreign intelligence agency and brought in by an authorized user. Once the flash drive was placed in a computer, the malicious code spread throughout the DOD network undetected.[22] The virus was moved by flash drive to both the classified and unclassified networks.[23] The malicious code had the ability to silently give control of DOD servers to unknown adversaries. The DOD has not released the full extent of the compromise, but the malicious virus did have the ability to deliver information to adversaries clandestinely.[24] To clean and recover from what is described as the worst breach of United States military computers in history took 14 months and cost a billion dollars.[25]

Another major network defense information assurance vulnerability is information available on the internet. The internet has free password crackers, firewall hackers, and encryption-defeating tools. YouTube even has how-to videos to hack everything from traffic lights to Facebook accounts. The basic problem with network defense information assurance is that the internet was designed as an open sharing tool between universities. Network defense information assurance actions are attempting to secure an infrastructure that was designed to be open. Firewalls, anti-virus software, access control, and software patches are important aspects of network defense, but these measures are basically static in nature and cannot completely secure a network.

Network defense response actions are actions that are planned in response to a compromise. Network defense response actions can range from relatively benign to very aggressive. Similar to a static machine gun, a network defense response has no effect until someone gets into its field of fire. Preplanned responses range from relatively simple, like cleaning a virus off a computer, to very complicated, like network administrators setting up traps for hackers called "honey pots." Honey pots leave known vulnerabilities open on a network to collect intelligence on hackers. Hackers and attackers leave "signatures" that are characterized and filed similar to a finger print database. The signature database assists in attribution of future attacks. Some network defense response actions operations are offensive in nature and may actively counterattack the source of the attack.

Figure 1: Network defense uses passive measures like barbed wire and sandbags as well as response actions to defend, like firing a machine gun at an attacker.

Network exploitation operations are designed to gain access to information or to actually control computer systems.[26] Cyber espionage is a form of network exploitation that is currently a low risk, high-gain activity. There are hundreds of exploitation programs and just one mid-range program exploits globally fifty times the amount of data that was taken in the Wiki leaks espionage case.[27]

China, for example, has been accused of performing massive network exploitation operations against the United States Government and private industry. Attribution is difficult

with network exploitation because even when perpetrators have been identified geographically, nations can claim that the exploitation was from a nongovernmental hacker acting independently. Whether state sponsored or not, Chinese hackers have been stealing intellectual research and development projects, software source code, and manufacturing know-how from the United States for years.[28] The loss of intellectual property and government secrets due to network exploits has resulted in significant erosion of the technological advantages previously enjoyed by the United States.

Network attack is very similar to network exploitation. The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime. The difference is what the operator at the attacking keyboard does with the information.[29]

An example of a successful network attack occurred in September of 2007, when Israel bombed a nuclear facility in Syria, which was reportedly constructed by North Koreans to make nuclear weapons. Syria had spent billions of dollars on its air defense systems, but the night of the attack nothing appeared on the Syrian radar screens except the images that Israel put there during the attack.[30] As Richard Clarke stated in his book, *Cyber War*, "Israel had owned Damascus's pricey air defense network."[31] The Israeli Air force flew planes to targets in Syria without ever being detected by Syrian air defenses because of a successful Israeli network attack. The integration of a network attack, with a conventional military attack made the operation an overwhelming success. The nuclear facility was destroyed and Syrian nuclear intentions were delayed indefinitely.[32]

EW is the second operational capability in cyber warfare. The DOD definition of EW is any military action that involves the use of the electromagnetic spectrum to include directed

energy to control the electromagnetic spectrum to attack an enemy.[33] EW can be broken into three components: electronic attack, electronic protection, and EW support.

The use of wireless internet and cellular telephone networks has created a wide range of opportunities for the combination CNO and Electron Warfare. A good example is again the Israeli bombing of Syria's nuclear reactors. This network was "owned" by Israel just long enough to conduct a bombing raid on the Syrian nuclear plant, and after the mission the network itself was undamaged. This ability to influence the command and control picture of the enemy is a relatively new capability created by joining the electronic attack and network attack capabilities.

An example of a failure in electronic protection was the recent loss of RQ-170 stealth drone over Iran. Iran claims that the RQ-170 was electronically attacked and hijacked by Iranian forces.[34] This was an advanced attack that used the proper frequency and the correct cryptographic material to guide the aircraft; it is evident the aircraft was lacking the proper electronic protections. The failure in protection led to an unacceptable technological loss. The United States needs to continue to enhance its electronic protection measures.

To quote Sun Tzu, "Invincibility lies in the defense; possibility of victory in the offense." In the cyber domain the United States remains primarily defensive focused, but to ensure the safety of the nation the United States needs to continue to advance its doctrine to include offensive cyber operations. Currently, adversaries of the United States do not fear negative consequences from their cyber operations. The possibility of painful cyber or kinetic retribution attack must be understood by adversaries to appreciate that cyber actions may have severe consequences.

THE WEB IS THE NEWEST WEAPON

In June 2010 a computer virus named Stuxnet was discovered in Power Plants and factories around the world.[35] More complex than any virus ever seen, Stuxnet was designed to attack industrial systems referred to as supervisory control and data acquisition (SCADA), systems. Stuxnet had the ability to turn up the pressure inside nuclear reactors' centrifuge machines or switch off oil pipelines.[36] Stuxnet exploited system vulnerabilities that system creators were not aware of, referred to as "zero day exploits."[37] Zero day exploits are rare and extremely time-consuming to develop, because they create vulnerabilities that have not been identified. Viruses rarely have even one zero day exploit, but Stuxnet was so technologically advanced that it had four of these highly technical exploits.[38] Stuxnet is considered the most complex virus ever created, and Microsoft assessed that to create the virus took more than 10,000 man-hours.[39] This effort is widely believed to have required the support from a technologically advanced nation or state.

When Stuxnet was deployed, it was looking for a specific target; if it did not see its specific target, it would lay dormant. Stuxnet was a precision guided munition designed to attack the centrifuges that spin nuclear material at Iran's enrichment facilities.[40] This weapon had the potential of creating a nuclear incident; it attacked a civilian facility, and was made entirely out of software. Whoever designed and employed this code understood the danger, but continued despite the possibility of a nuclear incident. If this attack was a traditional kinetic attack, it would have been an act of war. However, since the definition of cyber warfare is unclear and cyber attacks are difficult to attribute, Iran did not declare war because they did not know who executed the attack. Intelligence experts report that 1,000 centrifuges in Iran's main enrichment facility, in Nantanz, had to be replaced after the Stuxnet attack,[41] delaying nuclear

production capability in Iran by two years. Stuxnet to date is completely non-attributable to any group, nation, or state.[42]

The weapon was relatively inexpensive to create, but Stuxnet is now a genie out of the bottle. The tremendously dangerous and sophisticated virus that successfully attacked a SCADA system is now available for free on the internet. The internet has tutorials on how to design and even employ Stuxnet. Therefore, it is a very safe assumption that a variation of Stuxnet code will most likely be re-used by another organization to attack another institution in the near future.

Now that the technology of Stuxnet is widely available, this weapon no longer requires a major financial investment or the backing of a nation state. It can now be copied and recreated easily. No fissile material or stealth technology is required, and it can be deployed at the speed of light. The proliferation of cyber weapon technology cannot be easily controlled; the technology is cheap and spreading to traditional powers such as Russia and China and to terrorist organizations. Cyber weapon development is not going to go away, it is going to proliferate. In order to protect the government, industry and its interests; the United States needs to adjust its current definition of the cyber world and develop doctrine for cyber war.

AWATING THE CYBER 9/11

Before the events on 9/11, terrorism was largely considered a crime problem handled by the law enforcement and the intelligence community.[43] Local police and the FBI would arrest terror suspects and the CIA was heavily engaged in intelligence collection against terrorist organizations. Terrorism was not a DOD focus of effort. The events of 9/11 changed the focus for the DOD, and the DOD now fills a major anti-terror role because of the ferocity of the 9/11 attacks.[44] Similar to 9/11, adversaries we face today will exploit the nation's cyber defenses in an effort to destroy the American way of life.

Cyber war has already begun. Its costs are low and its impacts can be great. The most target-rich country in the world is the United States, but the military networks are not the prime targets, the prime targets are in the civilian sector. Leon Panetta, the Secretary of Defense, warned "the next Pearl Harbor will be a cyber attack."[45] Just as the attack on Pearl Harbor finally galvanized the United States' government and public sectors after years of aggressive Japanese actions throughout the Pacific, Leon Panetta's warning is *deja vu*. State and non-state actors have been performing cyber operations against the United States at an alarming rate and the loss of intellectual property and United States Government secrets has weakened the United States defense posture and negated its technological advantages, but it seems that the "sleeping giant" of the United States is again awaiting a very public, catastrophic event before awakening. The reorganization of DOD capabilities and the integration of civilian capabilities will then almost certainly be called upon to challenge the evolving cyber world threat.

Defining critical infrastructure will be a responsibility of Congress, but a series of Presidential decision directives defined critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government,"[46] The definition of critical infrastructure will often need to be redefined by Congress as reliance on the cyber domain continues to grow in the United States.

In 2003, a software engineering glitch in FirstEnergy Incorporated software caused a power outage throughout the Northeast and Midwest United States and parts of Canada. In four minutes power was lost to 50,000,000 people.[47] This was not an attack; this was an inadvertent programming error.[48] However, if this had been an attack, the United States government would not have had the ability or authorities to provide assistance to FirstEnergy. The United States lacks the ability for cyber coordination between the government and the private industry.

Placing the DOD in charge of United States cyber defense will consolidate shared information about cyber attacks. A single point of information collection will create a cyber defense team approach between the private and public sectors. Attacks that occur in the private sector are rarely shared with the government. Even within the government, the .GOV and .MIL domains rarely share information on cyber attacks. Currently, the DOD operates and protects .MIL domain, the Department of Homeland Security (DHS) is responsible for protection of the .GOV domain, and each private sector entity is responsible for the defense of its own tiny piece of the .COM domain. There is no incentive for the private sector to reveal to the public sector the amount or types of cyber attacks that are occurring. Bank of America and most of the defense industrial base is not required and does not reveal the types and numbers of attacks that are occurring to their systems. They, in fact, are disincentivized because customers, investors, or government entities contracting for their services may lose confidence in the particular company's ability to defend themselves. Prior to a truly catastrophic event, the United States government needs to come to grips with the threat, create a legal framework and empower the DOD to mount a defense. The DOD is the most significant entity charged with the defense of the nation, and is the only entity that has the capacity to accomplish this huge task.

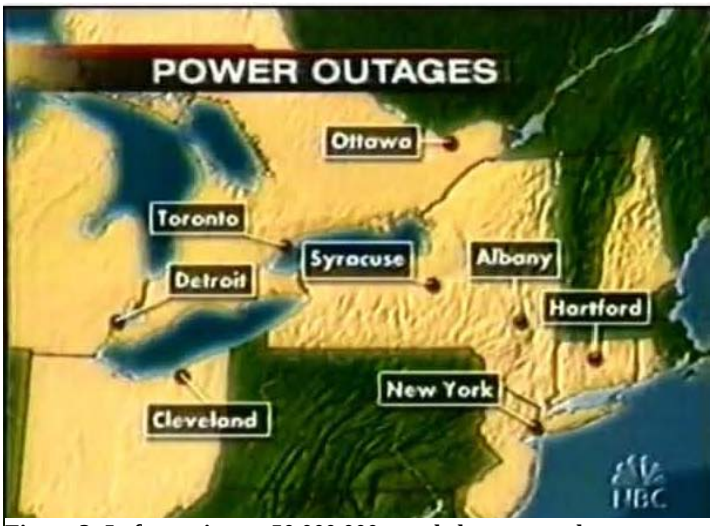


Figure 2: In four minutes 50,000,000 people lost power due to a cyber programming "error." It took over 30 hours to restore power. What if it were an attack? Yellow highlights the area of the power outage. ***Courtesy NBC***

WHY THE DOD

The DOD exists to protect the security of the United States. To defend against the ever increasing number and complexity of cyber attacks, the United States Government needs to identify the DOD as the nation's leader in cyber defense. The DOD has already created a new command named Cyber Command and co-located it in Fort Meade, Maryland with the National Security Agency (NSA). The combining of the NSA (the premier cyber collection and cyber defensive operation in the world) with the DOD (the premier offensive cyber capability in the world) leveraged existing cyber capabilities that could not be replicated because the cost of recreating these capabilities is prohibitive and the intellectual resources resident at these institutions would be extremely difficult to recreate. The integration of Cyber Command and NSA provides the people, the expertise, and the equipment required to defend the United States in cyber space. General Keith Alexander serves as the commander to both Cyber Command and NSA. The commander ensures the partnership is leveraging the capabilities of both commands.

Cyber Command integrates the existing pool of personnel, substantial funding, and is authorized to perform offensive cyber operations. Cyber Command draws its personnel from the private sector, government, and service components. NSA, the co-command with Cyber Command, employs over 800 PhDs and is the world's largest single employer of mathematicians.[50] The 24th Air Force, 10th Fleet (Navy), Marine Forces Cyber, and Army Forces Cyber provide personnel with expertise and experience in defending mission critical networks.[49] The nuclear command and control Emergency Action Network is one of the 15,000 networks that the DOD defends, making the DOD the largest cyber network in the world.[51] The DOD networks are located across hundreds of installations in dozens of countries around the globe.

Cyber Command Headquarters has a fiscal year 2012 budget of $159 million and the DOD has a technology budget of approximately $38 billion.[52] Cyber Command provides the nation an existing cyber defense capability, funding, and expertise that cannot be recreated or replicated.

Cyber Command has provided the .MIL domain with the most capable cyber defense in the world, but Cyber Command is not authorized to direct the security of the .GOV or .COM domains. Legal authorities and response actions need to be authorized before a cyber attack is launched. Attacks against the United States will occur at "net-speed" and defenders of the United States cyber domain require maneuver space and authorities. If an attack against the .GOV or .COM domains occurs, the attack will not stop while the United States debates authorities.

The technical expertise required to view, understand and coordinate actions in cyber space is very limited. General Alexander estimates that only about 1,000 people in the United States are currently qualified with the proper clearances, technical abilities, and certifications.[53] This small pool of trained and proficient "cyber warriors" are a high value commodity that are fought over between the public and private sectors. The current model of the private sector, which includes vital infrastructure, providing its own defense without government assistance does not leverage the limited workforce that exists in cyber defense. Designating the DOD as the lead for cyber defense will leverage the small pool of experts and assist in cyber collaboration.

The United States Code, Title 10 - Armed Forces, would need to be amended to allow the military to assume the lead on cyber defense in the United States. Congress has adjusted laws to allow the military to indirectly assist in fighting drug trafficking, natural disasters, and terrorist attacks. The exception to Title 10 would need to allow the DOD to perform cyber operations

domestically. This would provide the DOD the ability to protect U.S. national security interests in cyber space.

CYBER COP

In order to protect the financial systems, power grids, telecommunications, water supplies, intellectual property, and military communications of the United States, the United States Government will need to generate a comprehensive picture of cyber space. A cyberspace Common Operational Picture (COP) that fuses the public and private realms will provide the United States a tool that could be used to prevent, detect, and recover from attacks. The DOD needs to be provided the command structure, resources and authorities to monitor, enact and enforce security standards on the internet. This is a national security issue because it affects the nation's economy and national defense.

To effectively defend cyber space the United States needs to develop its situational awareness of the cyber domain. The United States government and private sector are interconnected in to the same commercial infrastructure. The cyber COP needs to be able to merge the government and private sector cyber picture to focus efforts on known and emerging threats and be able to provide the United States "cyber warriors" an ability to outmaneuver adversaries in the defense or on the attack.

The proposed cyber COP can be understood by dividing it in to blue, red and white feeds. Blue feeds would represent friendly devices that support our cyber networks.[54] Red feeds would represent threats to the network to include adversaries, physical damage, accidents or equipment failures.[55] White feeds would provide situational awareness of activities outside of the United States cyber domain, focusing on emerging threats to provide defenders a proactive intelligence capability.[56]

When armed forces select a position in the real world the focus is on selecting, capturing, and retaining key terrain. Similarly, the cyber COP will focus on key cyber terrain. The cyber terrain will need to be a prioritized list of key nodes that encompass the .GOV, .MIL and .COM domains. Visibility of the key cyber terrain will assist in situational awareness of cyber space. Situational awareness is vital for timely and effective cyber responses. Situational awareness of the air, land, sea, and space domains will also be vital. For example, a relatively simple Global Positioning System (GPS) denial of service in response to an attack could have dramatic unforeseen impacts on the commercial sector (e.g. shipping or aviation) or precision fires for the military.

In the past, the DOD has relied on units moving into position as an indication or warning that an imminent attack may occur. For example, China will likely reposition forces before attacking Taiwan. Learning of an imminent attack when forces are already in place is too late; Combatant Commanders need more time to prepare effective response actions. Future conflicts will be preceded by an increased amount of cyber activity. An example is the 2008 Russian invasion of Georgia that successfully coordinated cyber attacks with kinetic attacks. The cyber COP would be able sense traffic for anomalies that could provide indications or warnings that could push the Combatant Commander's timeline to the left.

The cyber COP would also assist in offensive cyber operations. Recent attacks on US corporations such as Google, the Nasdaq stock exchange, Lockheed Martin, Symantec, and many others has demonstrated the threat to the United States private sector. After a lengthy process of forensics some of the attacks were attributed to China and Russia. These attacks occur daily and the attackers do not fear any cyber retaliation. Retaliatory cyber tools exist; a cyber tool was recently developed by Japanese defense engineers.[57] The engineers developed a digital virus that

can track down, identify, and disable attacking systems. The United States Government needs to assist in the defense of key private sector industries by providing an offensive capability.

The framework for prioritization of fused information from the .MIL, .COM, and .GOV domains has been developed and is currently operational in the DOD. The DOD focuses on categorizing vulnerabilities, threat activities and their most likely consequences. The threat category and the severity of the threat drives resources, time and attention given to an identified problem. The fused cyber COP will alert the DOD of a threat to the vital national interests of the United States.

REGULATION REFORM REQUIRED

To protect the American people, the United States Government has placed many types of regulations on the nuclear industry, electrical industry, health care industry, financial industry, defense industry and government institutions, but has not created any meaningful regulations on cyber security. The United States Government has a responsibility to ensure that the government and private companies of "vital national interest" are compliant with current best practices of cyber security policies. The government needs to set and regulate standards with respect to encryption, protection of data and task the DOD with ensuring cyber security compliance.

Cyber security is currently in the Wild West era, where anything goes. There are no baseline requirements for cyber security and companies are free to decide for themselves what constitutes enough security, yet 73% of United States internet users have been the victim of a cyber crime.[58] According to MacAfee, the cost of cyber crimes globally has passed 1 trillion dollars because of lost intellectual property and damaged equipment.[57] The DOD reports that its networks are probed for weaknesses about 250,000 times an hour.[59] The growth and increased threat against e-commerce alone has made cyber-security essential for national defense.

The government has a responsibility to set regulations and ensure compliance of cyber security. The DOD, with collaboration from DHS, the Intelligence Community, and the private sector need to publish required baseline settings for firewalls, anti-virus software and encryption systems. Regulated and assured compliance of cyber security practices in key industries is a requirement for national security.

TO THE CLOUD

Cloud computing is fundamentally transforming the cyber security industry into a more cost effective and secure environment. With DOD oversight the United States government and critical infrastructure within the private sector can leverage and transition to a more secure and reliable cloud environment.

Currently Information Technology (IT) is generally internally managed by the government agencies and the commercial sector. Infrastructure costs for IT include hardware, maintenance, power and technical support personnel. Additional risks for the IT departments are the risks of fire, severe weather, earthquakes, terrorism, or utility outages. These costs overshadow and divert attention and funding from IT security. The risks and costs of operating independent IT departments were once necessary and led to the buildup of large disparate networks. The DOD network, for example, is now made up of 15,000 disparate networks with two million computers and 5 million devices requiring internet protocol addresses.[60]

The DOD network is an example of government and commercial networks in the United States; the DOD has the best visibility on its network of the three domains; .MIL, .COM and .GOV so it will be used as a sample. The DOD network architecture has grown into a collection of networks, systems, and software that nobody completely understands, making it virtually

impossible to protect and expensive to manage.[3] The cloud (a metaphor for the internet) provides applications, storage, and other services via a web browser. The computing resources are consolidated at a data center owned by a third party. The users have computer services provided like a utility. The users no longer need large in-house IT departments because the services are paid for as needed, similar to an electric utility bill. Users of the cloud do not require the physical location or personnel to configure servers to provide IT services.

Cloud computing is more secure than traditional network environments because it is centrally managed, which means that policies can be applied from the top and pushed out to ensure that the latest security patches are in place instantly. The current model of having 15,000 disparate networks requires the coordination with all 15,000 network owners and technicians to fix security settings. The sheer number of different networks makes security of the .MIL difficult. Cloud Computing centralizes many users so a small team of security professionals have larger impacts. The cloud provides an ability to apply security controls to an entire network instantaneously and this provides improved security. A well managed cloud environments leads to an improved security environment.

Many of the major suppliers of corporate IT, including Microsoft, IBM, Sun, and Oracle, are investing billions of dollars and battling to position themselves as dominant suppliers of "Web services" to turn themselves, in effect, into utilities.[61] These large-scale cloud computing companies have built multiple redundant datacenters the size of 10 football fields and located them around the world.[62] Each data center has tens of thousands of state-of-the-art servers. The infrastructure to support the data centers includes fire protection, environmental controls, emergency power backups, and independent fuel incase of rolling power outages or natural disasters. The data centers have high speed fiber optic connections to the internet and to other

data centers. These connections provide the data centers capabilities. Teams of engineers work to ensure the availability of the data centers and to ensure the customer's cloud is performing at optimal performance and security.

Cloud computing is making much of the cyber world a utility, much like electricity. Early power generation systems were complex, proprietary, and unsafe. So with the backing of the government, public utilities developed infrastructure to provide safe, standardized, and reliable infrastructure. In an effort similar to commoditization of electricity, the government needs to encourage the movement of vital national cyber elements from internal IT departments to secure regulated cloud computing companies that are in compliance with national standards. This move will make the nations vital national interest more secure, more reliable, and more cost effective.

CONCLUSION

Today, the only entity not in the .COM and .GOV domains is the DOD.[63] China, Russia, terrorist organizations, criminal gangs, teenage hackers, and anarchists have already paved roads into these domains as well as the .MIL domain. The United States needs to develop a cyber strategy that protects government and extends protection to the nation's privately owned critical infrastructure. Cyber security is a team sport that requires players from the private and public sectors to share information about vulnerabilities. The aggregated information will improve situational awareness and will be the basis for a cyber COP. Improved collaboration will be mutually beneficial for both the private and public sectors.

The DOD should be given the authority to lead the United States in cyber defense. An amendment to United States Code, Title 10 – Armed Forces, to allow the DOD the ability to perform cyber investigations would leverage the DOD's intellectual capital, technical expertise,

equipment, and funding that cannot be recreated or replicated; therefore, selecting the DOD would be an efficient use of the nation's resources. The DOD already has some authorities to offensively respond to protect the United States in the cyber domain. State and non-state actors currently penetrate and exploit American cyber space with no fear of retaliatory strikes. The DOD is prepared and could provide a near real time offensive response to cyber warfare.

The amount of illegal money being made in cyber space has now eclipsed the drug trade.[64] The lack of regulated baseline standards with respect to firewalls, anti-virus software and encryption systems has cost an estimated 1 trillion dollars worldwide.[65] The United States must enforce regulations on cyber security to secure the future of the nation. The United States stores its wealth, intellectual property, and operates its critical infrastructure in cyber space. Regulations exist in the nuclear industry, the financial industry, the defense industry, water and electricity utility industries, but not in the security of the cyber backbone that enables all of these industries. The definition of critical infrastructure would need to be created by congress but generally should encompass cyber systems required for supporting the economy and government of the United States.[66] Cyber security is a matter of national defense, and DOD should be given authorities to set baseline cyber security regulations to defend public and critical private sector industries.

The current model of networking in the United States is indefensible; the DOD alone has 7 million devices working off of 15,000 disparate networks managed independently.[67] Recent technological innovations such as "cloud computing" must be leveraged to create a more secure, more reliable, and more cost effective cyber space. For example, the collapsing of the DOD's 15,000 disparate networks to a cloud environment will provide the DOD the ability to react to

threats at ”net-speed.” This model must be used and coordinated with critical public and private sectors.

The threats posed in the cyber domain are an existential threat to the security and prosperity of the nation. Currently the United States does not have an organization that has the capabilities or authorities to oversee cyber security for the U.S. Government and the U.S. private sector. To defend against the ever increasing number and complexity of cyber attacks, the United States Government needs to identify the DOD as the nation’s lead in cyber defense and enhance its authorities to fill that role.

End Notes

[1.] Daniel Kuehl, interview by Major Cliff Magee. *NDU Chair Cyber and I/O* (January 12, 2012).

[2.] Daniel Kuehl interview

[3.] Bryan Krekel. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* U.S. - China Economic and Security Review Commission, McLean, VA: Northrop Grumman, 2009. P. 41

[4.] Ibid P. 42.

[5.] Richard Clarke. "China's Cyberassault on America." *Wall Street Journal*, June 15, 2011. P. 59

[6.] Bryan Krekel. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* U.S. - China Economic and Security Review Commission, McLean, VA: Northrop Grumman, 2009. P. 43

[7.] Richard Clarke. "China's Cyberassault on America." *Wall Street Journal*, June 15, 2011. http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html

[8.] Ibid http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html

[9.] David Fahrenkrug, , interview by Harold Channer. *Guest Lt. Col. David T. Fahrenkrug Chief Strategist 8th Air Force* (April 17, 2008).

[10.] David Fahrenkrug interview

[11.] Keith Alexander, General Cyber command interview by PhD, Vice President, URI Reseach and Economic Development University of Rhode Island Peter Alphonso. "*Cyber Security Symposium"* (May 3, 2011). (48:44)

[12.] B.G. Kutais, *Internet Policies and Issues.* Hauppauge, New York 11743: Nova Science Publishers, Inc, 2002. P.2

[13.] Joint Chiefs of Staff, *Joint Publication 1*. Washington DC: DOD, 2009. P. I-7

[14.] David Fahrenkrug interview

[15.] Government Accountablility Office. *Definitions, Focal Point.* Washington DC, July 29, 2011. P. 2

[16.] Ibid P. 2

[17.] Ibid P. 2

[18.] SANS Institute (Internet Security Trainint) *20 Critical Security Controls.* Mobile Certification Courses: SANS, 2012.

[19.] Symantec. *Symantec Report Shows No Slowdown in Cyber Attacks.* Research, Mountain View, Califonia: Symantec, 2010.

[20.] William J. Lynn III, Speech *Defending a New Domain.* Cyber Security, Washington D.C.: Department of Defense, 2010.

[21.] William J. Lynn III Speech

[22.] William J. Lynn III Speech

[25.] Eric Chambrow. *Gov Info Security.* November 8, 2011. http://www.govinfosecurity.com/blogs.php?postID=1115 (accessed February 20, 2012).

[26.] Government Accountablility Office. *Definitions, Focal Point.* Washington DC, July 29, 2011.

[27.] Keith Alexander. General Cyber command interview by PhD, Vice President, URI Reseach and Economic Development University of Rhode Island Peter Alphonso. "*Cyber Security Symposium"* (May 3, 2011). (1:01:20)

[28.] Bryan Krekel. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* U.S. - China Economic and Security Review Commission, McLean, VA: Northrop Grumman, 2009. P. 57

[29.] Government Accountablility Office. *Definitions, Focal Point.* Washington DC, July 29, 2011. P.2

[30.] Richard Clarke. *Cyber War.* New York: Harper Collins Publishing, 2010. P. 5

[31.] Ibid. P. 5

[32.] Ibid. P. 5

[33.] Joint Chiefs of Staff. *Joint Publication 3-13.1.* Washington DC: DOD, 2007 P. V.

[34.] Scott Peterson. *The Christian Science Monitor.* December 15, 2011. http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (accessed February 15, 2012).

[35.] Ryan Naraine. "Stuxnet attackers user 4 Windows zero-day exploits." *ZD Net.* September 14, 2010. http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347 (accessed January 30, 2011).

[36.] Ibid P. 1

[37.] Ibid P. 1

[38.] Ibid P. 2

[39.] Michael Bame. "About Defense.Com." *About Defense.Com.* December 6, 2010. http://defense.about.com/b/2010/12/06/stuxnet-virus-targets-iran-cyber-warfare.htm (accessed January 30, 2011).

[40.] Ibid P. 1

[41.] Atika Shubert. "CNN." *CNN.* November 8, 2011. http://articles.cnn.com/2011-11-08/tech/tech_iran-stuxnet_1_stuxnet-centrifuges-natanz-facility?_s=PM:TECH (accessed January 30, 2012).

[42.] Ibid P. 2

[43.] Robert B Bruce, interview by Major Cliff Magee. *Professor Marine Corps University* (February 8, 2012).

[44.] Robert B. Bruce interview

[45.] Lisa Daniel. "Panetta: Intelligence Community Needs to Predict Uprisings." *American Forces Press Service*, February 11, 2011.

[46.] Michael V. Hayden, “Black Hat USA 2010: Cyber war: Are we at war? And if we are, how should we fight it?” *YouTube,* http://www.youtube.com/watch?v=XXnIvBBASLI&feature=relate (accessed March 6, 2011)

[47.] Michael F. Hordeski, *Megatrends for Energy Efficiency and REnewable Energy.* Lilburn, Georgia: Fairmont Press, 2011. P.238

[48.] Ibid

[49.] Keith Alexander, General Cyber command interview by PhD, Vice President, URI Reseach and Economic Development University of Rhode Island Peter Alphonso. "*Cyber Security Symposium"* (May 3, 2011). 1:16:32

[50.] Keith Alexander , General Cyber command interview by PhD, Vice President, URI Reseach and Economic Development University of Rhode Island Peter Alphonso. "*Cyber Security Symposium"* (May 3, 2011). 1:16:32

[51.] Teresa Takai, (DOD CIO). "The DoD Information Enterprise." *Chips Magazine*, October to December 2011.

[52.] Teresa Takai, (DOD CIO). "The DoD Information Enterprise." *Chips Magazine*, October to December 2011.

[53.] Tom Gjelten. "Cyberwarrior Shortage Threatens U.S. Security." *NPR*, July 19, 2010: http://www.npr.org/templates/story/story.php?storyId=128574055

[54] John Davis Brigadier General U.S. Cyber Command, interview by AFCEA. *AFCEA Cyber Situational Awareness* (February 2011).

[55] John Davis interview

[56] John Davis interview

[57] George V. Hulme, *Data Protection.* January 4, 2012. http://www.csoonline.com/article/697365/government-engineers-actively-plan-for-cyberwar (accessed February 15, 2012).

[58.] Keith Alexander, General Cyber Command, interview by AFCEA. *AFCEA HS-General Alexander Keynote-Feb 2011* (February 2011). (12:48)

[59.] Keith Alexander, General Cyber Command, interview by gov2 Summit. *Gov 2.0 Summit 2010: General Keith Alexander, "U.S. Cybersecurity Policy, Strategy..."* (Sep 7, 2010). (2:30)

[60.] Teresa Takai, (DOD CIO). "The DoD Information Enterprise." *Chips Magazine*, October to December 2011. P. 11

[61.] Nicholas Carr. *The Big Switch, Rewiring the World, From Edison To Google.* New York: Houghton Mifflin Company, 2008. P. 13

[62.] Ibid P. 60

[63.] Keith Alexander, General Cyber Command, interview by AFCEA. *AFCEA HS-General Alexander Keynote-Feb 2011* (February 2011). (35:36)

[64.] Keith Alexander interview

[65.] Keith Alexander interview

[66.] Takai, Teresa (DOD CIO). "The DoD Information Enterprise." *Chips Magazine*, October to December 2011.

[67.] Michael V. Hayden, “Black Hat USA 2010: Cyber war: Are we at war? And if we are, how should we fight it?” *YouTube*, http://www.youtube.com/watch?v=XXnIvBBASLI&feature=relate (accessed March 6, 2011)

Bibliography

Alexander, Keith, General Cyber command interview by PhD, Vice President, URI Reseach and Economic Development University of Rhode Island Peter Alphonso. "*Cyber Security Symposium"* (May 3, 2011).

Alexander, Keith General Cyber Command, interview by AFCEA. *AFCEA HS-General Alexander Keynote-Feb 2011* (February 2011).

Alexander, Keith General Cyber Command, interview by gov2 Summit. *Gov 2.0 Summit 2010: General Keith Alexander, "U.S. Cybersecurity Policy, Strategy..."* (Sep 7, 2010).

Asmus, Ronald. *A Little War That Shook The World.* New York: Macmillan, 2010.

Bame, Michael. "About Defense.Com." *About Defense.Com.* December 6, 2010. http://defense.about.com/b/2010/12/06/stuxnet-virus-targets-iran-cyber-warfare.htm (accessed January 30, 2011).

Bruce, Robert PhD, interview by Major Cliff Magee. *Professor Marine Corps University* (February 8, 2012).

Carr, Jeffery. *Cyber Warfare.* Sebatopol California: O'Reilly, 2010.

Carr, Nicholas. *The Big Switch, Rewiring the World, From Edison To Google.* New York: Houghton Mifflin Company, 2008.

Chambrow, Eric. *Gov Info Security.* November 8, 2011. http://www.govinfosecurity.com/blogs.php?postID=1115 (accessed February 20, 2012).

Clarke, Richard. "China's Cyberassault on America." *Wall Street Journal*, June 15, 2011.

Clarke, Richard. *Cyber War.* New York: Harper Collins Publishing, 2010.

Daniel, Lisa. "Panetta: Intelligence Community Needs to Predict Uprisings." *American Forces Press Service*, February 11, 2011.

Davis, Harold. *Building REsearch Tools with Google for DUMMIES.* Hoboken: Wiley Publishing, 2005.

Davis, John A Brigadier General U.S. Cyber Command, interview by AFCEA. *AFCEA Cyber Situational Awareness* (February 2011).

Dunigan, James. "The Politician Class Carriers Evolve." *Strategy Page*, April 11, 2009.

Fahrenkrug, David, interview by Harold Channer. *Guest Lt. Col. David T. Fahrenkrug Chief Strategist 8th Air Force* (April 17, 2008).

GJELTEN, Tom. "Cyberwarrior Shortage Threatens U.S. Security." *NPR*, July 19, 2010: http://www.npr.org/templates/story/story.php?storyId=128574055.

Google. *Google Flu.* January 30, 2012. http://www.google.org/flutrends/ (accessed January 30, 2012).

Hordeski, Michael F. *Megatrends for Energy Efficiency and REnewable Energy.* Lilburn, Georgia: Fairmont Press, 2011.

Hulme, George V. *Data Protection.* January 4, 2012. http://www.csoonline.com/article/697365/government-engineers-actively-plan-for-cyberwar (accessed February 15, 2012).

Joint Chiefs of Staff. *Joint Publication 1.* Washington DC: DOD, 2009.

Jones, Brett. "Loss of plane peels back layer in U.S.-Iran spying." *USA Today*, December 12, 2011.

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* U.S. - China Economic and Security Review Commission, McLean, VA: Northrop Grumman, 2009.

Kuehl, Doctor Dan, interview by Major Cliff Magee. *NDU Chair Cyber and I/O* (January 12, 2012).

Kutais, B.G. *Internet Policies and Issues.* Hauppauge, New York 11743: Nova Science Publishers, Inc, 2002.

Lynn III, William J. *Defending a New Domain.* Cyber Security, Washington D.C.: Department of Defense, 2010.

Naraine, Ryan. "Stuxnet attackers usen 4 Windows zero-day exploits." *ZD Net.* September 14, 2010. http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347 (accessed January 30, 2011).

Office, Government Accountablility. *Definitions, Focal Point.* Washington DC, July 29, 2011.

Peterson, Scott. *The Christian Science Monitor.* December 15, 2011. http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (accessed February 15, 2012).

Rhodes, Ron. *Cyber Meltdown.* Eugene, Oregon: Nova Science Pub, 2011.

Sanders, Sam. "Middle East and North Africa in Turmoil." *Washington Post*, Novermber 2011.

SANS Institute (Internet Security Trainint) *20 Critical Security Controls.* Mobile Certification Courses: SANS, 2012.

Shubert, Atika. "CNN." *CNN.* November 8, 2011. http://articles.cnn.com/2011-11-08/tech/tech_iran-stuxnet_1_stuxnet-centrifuges-natanz-facility?_s=PM:TECH (accessed January 30, 2012).

Symantec. *Symantec Report Shows No Slowdown in Cyber Attacks.* Research, Mountain View, Califonia: Symantec, 2010.

Takai, Teresa (DOD CIO). "The DoD Information Enterprise." *Chips Magazine*, October to December 2011.

Whitney, Lance. *CNET News.* January 18, 2012. http://news.cnet.com/8301-1023_3-57360925-93/internet-now-active-with-2.1-billion-users/ (accessed January 30, 2012).

Williams, Brigadier General Brett T. "The Imperative for Shaping CyberSpace." *ITEA Journal*, December 2010: 440-441.